SOPHOS
Cybersecurity delivered.

主动对手指南 2022

2021 年在事件响应前线见到的网络攻击者行为、战术和工具

作者 John Shier，CTO 办公室资深安全顾问

Sophos 白皮书 2022 年 6 月

介绍

帮助企业抵御快速发展、越来越复杂的网络威胁的挑战很大。对手不断调整和进化自己的行为与工具组合，利用新的漏洞和误用日常 IT 工具避开侦测，领先安全团队一步。

企业的 IT 和安全运行专家可能难以跟上对手采用的最新方法。尤其是涉及多个罪犯的针对性活跃攻击，例如初始访问代理 (IAB) 攻破目标后，将访问权出售给勒索软件团伙用于其攻击。

主动对手指南 2022 详细接受 Sophos 前线事件响应人员在 2021 年见证的主要对手、工具和攻击行为。本指南延续主动对手指南 2021，介绍攻击局面如何继续演变。

目的是帮助安全团队了解对手在攻击过程中所做的操作，如何在自己的网络上发现和抵御此类活动。

结果基于 2021 年 Sophos 快速响应团队调查的事件数据。如果可行，将与主动对手指南 2021 概述的事件响应结果对比数据。

事件响应人口统计 2021

报告基于针对各行业领域所有规模企业的 144 个事件，这些企业分布在美国、加拿大、英国、德国、意大利、西班牙、法国、瑞士、比利时、荷兰、奥地利、阿联酋、沙特阿拉伯、菲律宾、巴哈马、安哥拉和日本。

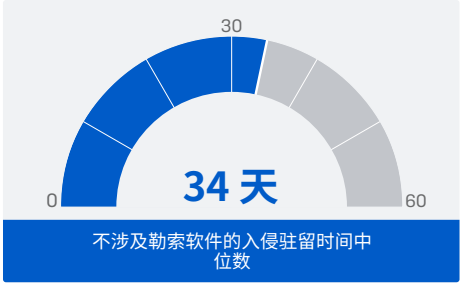
最具代表性的行业包括制造 (17% 的事件响应案例来自此行业)，接下来是零售 (14%)、医疗 (13%)、IT (9%)、建筑施工 (8%) 和教育 (6%)。本报告末尾的数据表格提供更多信息。

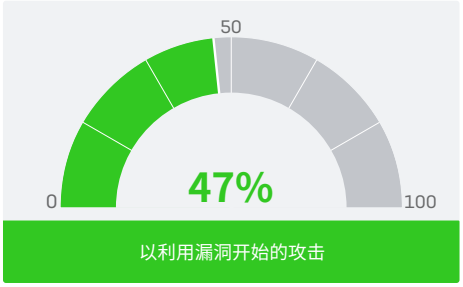
仪表板：2021 年主动攻击解析

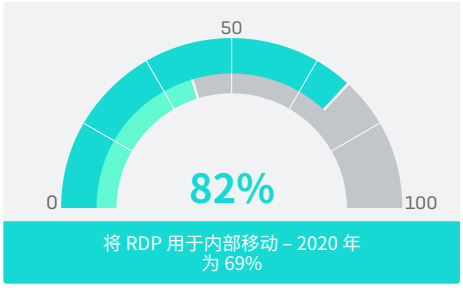
2021 年最具影响力的 2 个网络威胁事件发生在 3 月和 8 月，报告 Microsoft Exchange 服务器的 ProxyLogon 和 ProxyShell 漏洞。据 CISA 和其他政府安全机构表示，对手深入利用了 ProxyLogon/ProxyShell 缺陷。所以 Sophos 在 2021 年调查的大量事件与此相关并不让人意外。

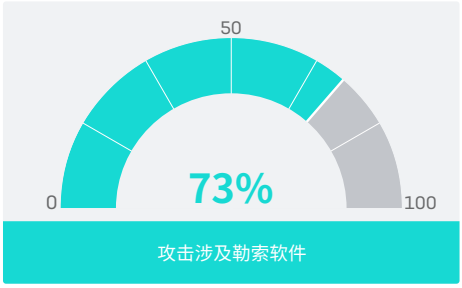
仪表板：2021 年主动攻击解析

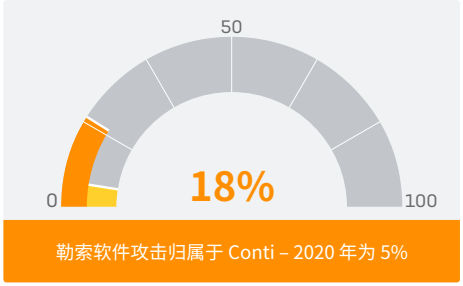
来自事件响应调查的重要结果

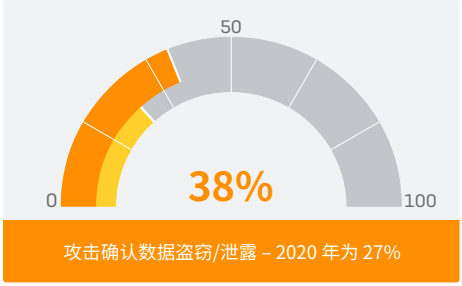












很可能还有更多 ProxyLogon/ProxyShell 外泄目前还处于未知状态，受害者已经被植入 web shell 和后门用于持续访问，但现在处于静默等待状态，直到使用权被使用或出售。

这导致了 2021 年改变网络威胁蓝图的另一个重要变化：初始访问代理 (IAB) 的影响力和威力增加。

IAB 的成功依赖首先攻破目标，取得可以出售的访问权。因此，IAB 往往很快出现在新报告的缺陷范围中，希望在大范围打补丁之前攻破目标。他们的目的是在受害者中立足，可能做一些初始探索工作以了解资产价值 – 然后出售给其他对手，例如勒索软件运营商，用于攻击，有时候在初始侵入数月后才进行。

Sophos 2022 威胁报告中强调，IAB 的崛起反映网络威胁市场的攻击越来越“专业化”，专业服务供应商数量越来越多。不断发展的勒索软件即服务 (RaaS) 行业是这一趋势的另一个例子。

最后，2021 事件响应调查中发现的鉴证证据揭示，包括 IAB、勒索软件团伙、加密货币矿机以及偶尔多个勒索软件运营商在内的多个对手同时将一个企业作为目标。这个发展将在 2022 年及以后继续改变网络威胁蓝图。

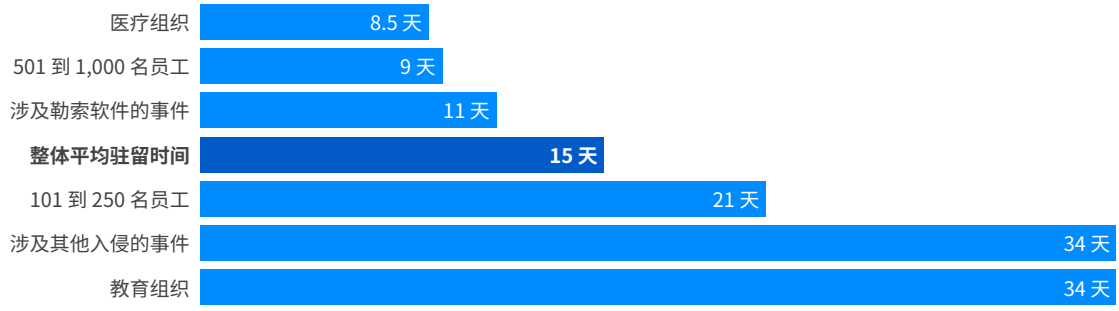
入侵者用于受害者网络的时间长度增加，可能因此类活动导致。长期留在受害者网络（有时候同时）的其他对手包括僵尸网络搭建者和恶意软件投放平台或 dropper。

下面将更加详细讨论这些发展。

看不见的入侵者

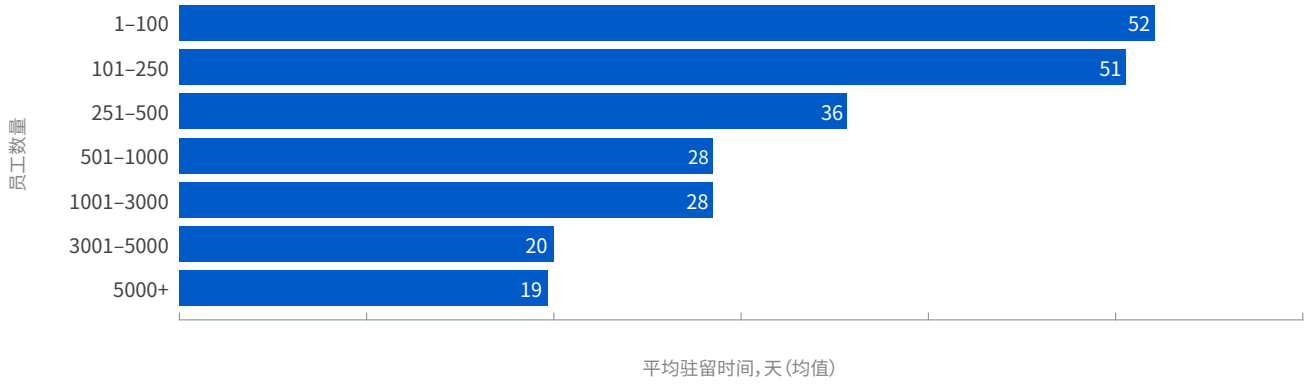
事件数据显示，2020 到 2021 年，平均驻留时间中位数增加约三分之一，从 11 天增加到 15 天。出现显著差异，勒索软件攻击的驻留时间更短，平均约 11 天（2020 年为 18 天），涉及其他入侵的驻留时间明显延长，驻留时间中位数为 34 天。

平均入侵者驻留时间（中位数）差异



如上所示，更长的驻留时间反映涉及 IAB。对于小企业或行业领域，如教育（平均入侵者驻留时间 34 天），更长的驻留时间还说明内部 IT 安全人员主动主动、调查和响应可疑提醒与潜在威胁的难度。

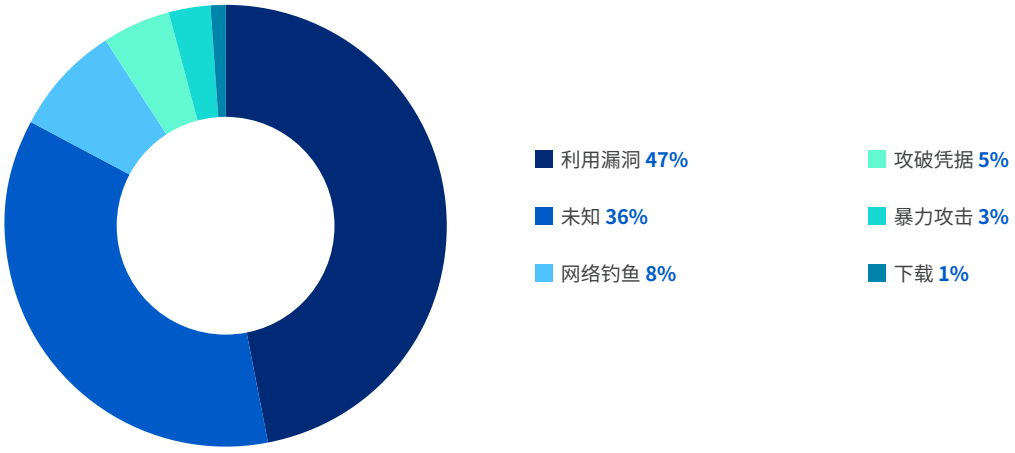
按公司规模划分的入侵者驻留时间（平均值）



攻击的根本原因

并不是始终可以或者可以轻松发现攻击的根本原因。有时候攻击者故意删除活动证据，有时候 IT 安全团队在响应者到达前擦除或重新镜像被攻破的计算机。但是，证据表明，在 Sophos 调查的事件中，利用未打补丁的漏洞 – 如 ProxyLogon 或 ProxyShell – 是 2021 年调查的近一半 (47%) 网络事件的根本原因。

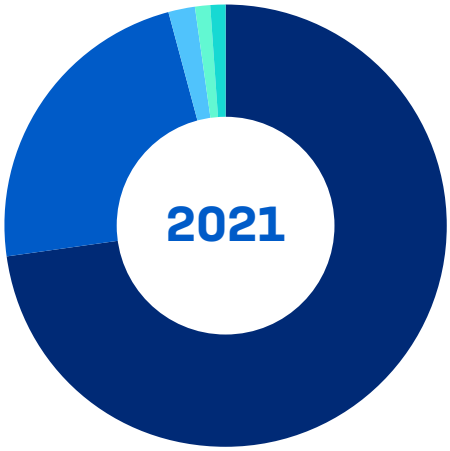
攻击的根本原因



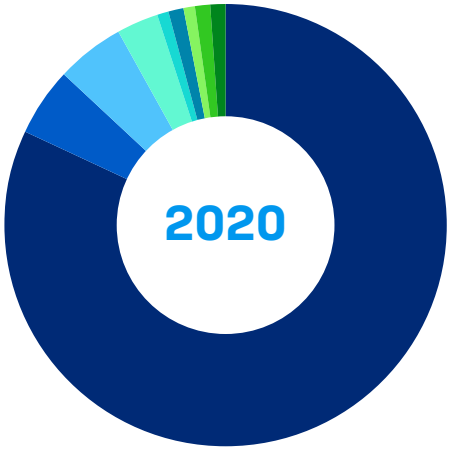
主要攻击类型

勒索软件通常发布在 IT 安全团队可以看到攻击的时候。因此，2021 年 Sophos 响应的 73% 的事件涉及勒索软件并不令人意外。勒索软件还是 2020 年最流行的攻击类型，为 82%（数字越高可能说明数据集越小）。对于数据泄露（占事件的 1%），事件响应者认为这些可能是在勒索软件攻击中发现但及时消除的。

攻击类型



- 勒索软件 **73%**
- 其他入侵 **23%**
- 加密货币矿机 **2%**
- 数据泄露 **1%**
- Dropper **1%**



- 勒索软件 **82%**
- 未知 **5%**
- 泄露 **5%**
- 加密货币矿机 **3%**
- 木马/Dropper **1%**
- 银行木马 **1%**
- Wiper **1%**
- 渗透测试/攻击工具 **1%**
- 阻止 **1%**

事件响应调查发现的第二大流行攻击类型是广义的“其他入侵”，占事件的 23%。对于本报告，“其他入侵”定义为没有导致勒索软件或其他跟踪攻击类型的入侵。

入侵通常是利用未打补丁的漏洞的结果，例如 ProxyLogon 和 ProxyShell，还包括误用远程访问服务或不安全的 VPN、帐户凭据失窃或安全疏忽（例如对互联网打开进入点）。

关键是在将主要恶意载荷投放到目标前，侦测并消除入侵。可以合理假定，部分（即使不是大多数）入侵属于 IAB：尚未出售给其他对手的“保管”访问权。如果尚未侦测到入侵，可能很多已经继续变为勒索软件攻击。

加密货币矿机是主要攻击类型，占调查事件的 2%。恶意加密货币框架的存在通常通过对系统性能的影响发现，因为非法货币挖矿占用计算机计算能力。有人可能更愿意把加密货币框架视为较低级别的小威胁，但事实上它们出现在网络中已经证明这是一个存在漏洞的入口点，可以成为更严重威胁的跳板。

这也适用于普遍意义的 dropper 和恶意软件投放系统，设计为向目标系统投放、加载或安装其他恶意载荷。他们实现被发现的攻击，为其他恶意模块如后门或勒索软件提供平台。因此，防御者需要像对待大型勒索软件系列一样，认真对待 dropper 和恶意软件投放系统的存在，包括 Trickbot、Emotet 和其他，因为他们往往是更大规模攻击的前奏。

拥挤的赛场

攻击类型不是互相排斥的。正如前文提到的，多个对手（包括 IAB、勒索软件团体和加密货币矿机）可以同时出现在一个目标网络中。

例如，加密货币框架是占事件响应案例仅 2% 的主要攻击类型，同时占勒索软件事件的 7%。加密货币矿机通常扫描并移除受感染网络的其他矿机，但可以与其他威胁如勒索软件很好地共存。

Sophos 在 2021 年报告的同时攻击事件包括一个涉及 Atom Silo 勒索软件和两个加密货币矿机的攻击，一个涉及 Netwalker 和 REvil 的双重勒索软件攻击。此趋势在 2022 年继续。

主动工具箱

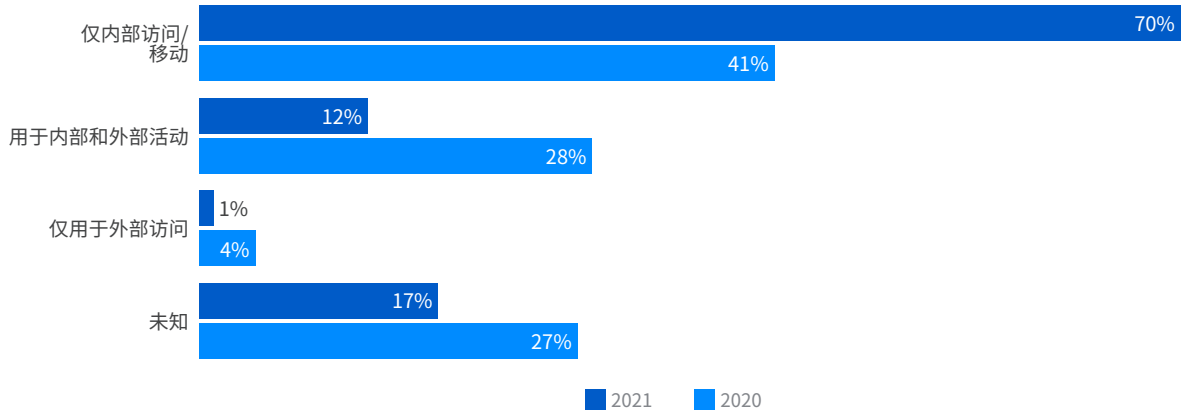
远程桌面服务是一个主要内部威胁

RDP 占攻击的至少 83%，比 2020 年增加（占攻击的 73%）。内部使用占案例的 82%，外部使用为 13%。而在 2020 年分别为 69% 和 32%。

但是，攻击者使用 RDP 的方式值得注意。在涉及 RDP 的事件中不到四分之三 (70%)，工具仅用于内部访问和横向移动—，相比 2020 年的 41% 显著增加。

用于外部访问的 RDP 在案例中仅占 1%，低于 2020 年的 4%；仅 12% 的攻击显示攻击者将 RDP 用于外部访问和内部移动，不到 2020 年的一半（之前为 28%）。

攻击者使用远程桌面协议 (RDP)



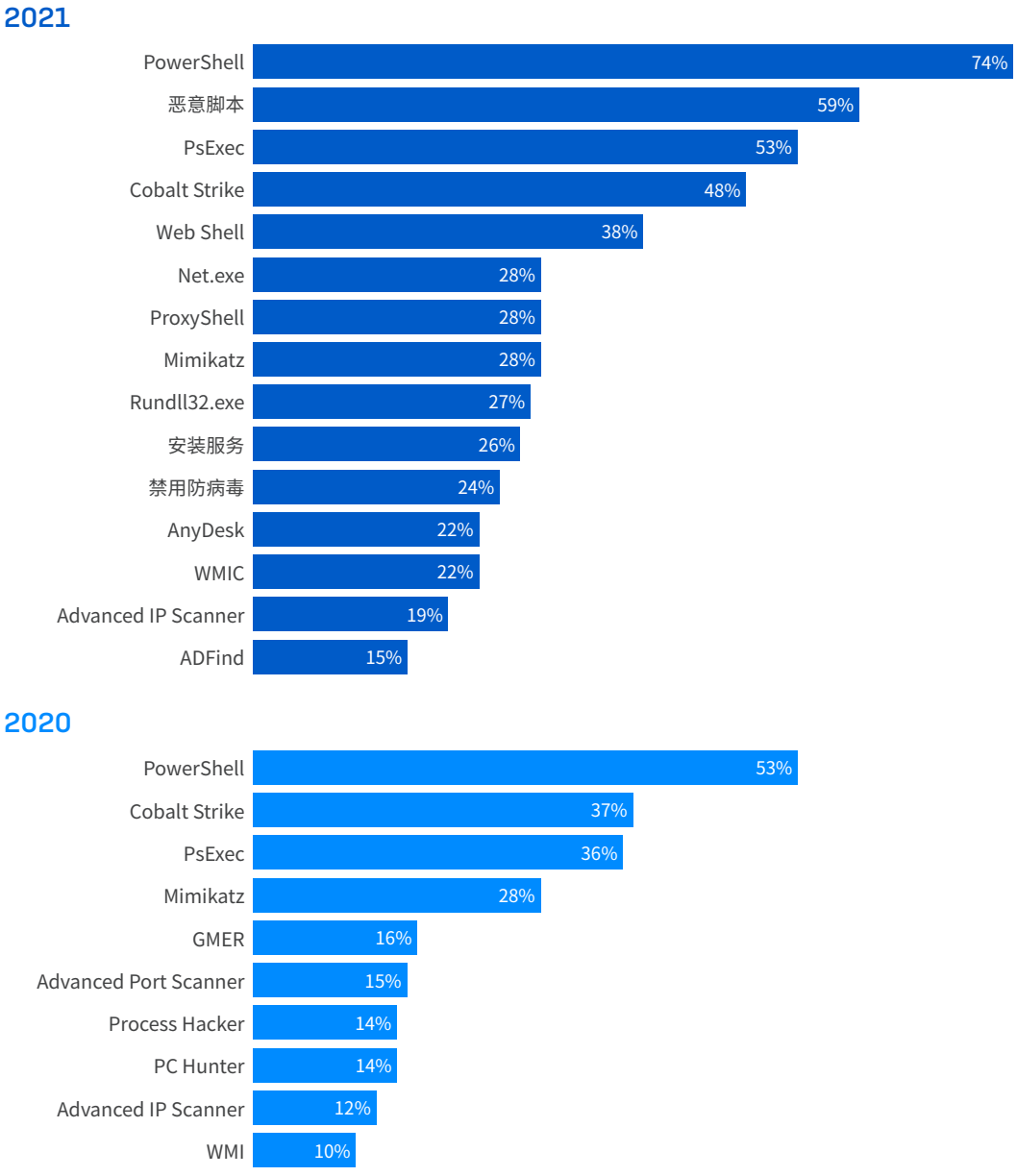
将 RDP 用于外部访问的下降可能体现了安全改进，包括禁用服务。但是，RDP 仍然在外围设施以内广泛可访问，加固此访问权应是安全团队的关注焦点。

2021 年的攻击工具集

下图显示“制作物”，包括 2021 年攻击者工具集中最可能出现的工具、技术和服务。其中许多还可供 IT 专业人员用于善意用途。对手熟悉这些制作物，因为可以用于开展凭据盗窃、发现、横向移动和恶意软件执行等活动，同时与无害的日常 IT 活动混淆在一起。

制作物的数量和性质凸显防御者在区分网络上的恶意和合法活动时面临的挑战。

攻击中用到的主要制作物



深入了解攻击中最常用的制作物，可以揭示 2021 年网络攻击的典型局面。

组成工具集的制作物

事件响应调查中确定的制作物可以分为三类：合法和黑客工具、Microsoft binaries 以及其他制作物（脚本、技术、服务等）。

事件响应调查共发现 525 个不同制作物，远高于 2020 年的 132 个（但样本基数更大），包括 209 个合法和黑客工具，107 个 Microsoft binaries 以及 209 个其他制作物。

合法和黑客工具

这些包括用于协助攻击的软件。Cobalt Strike (48%) 和 Mimikatz (28%) 依旧是 2020 年的前两位，之后依次是 AnyDesk (22%)、Advanced IP Scanner (19%) 和 ADFind (15%)。相比 2020，Cobalt Strike 的份额增加（之前为 37%），Mimikatz 保持稳定（保持在 28%），三个新工具进入前五。

Cobalt Strike 是一款商用漏洞攻击工具组合，设计帮助安全团队重建多种攻击场景。攻击者尝试在受感染的计算机上建立 Cobalt Strike“信号塔”后门。信号塔可以配置为执行命令，下载，执行其他软件，将命令中继到目标网络内安装的其他信号塔，与 Cobalt Strike 服务器反向通信。应立刻调查网络上侦测到的任何 Cobalt Strike。

第二常见的工具 **Mimikatz** 最初同样设计为进攻性安全工具，可以盗窃密码和其他帐户凭据用于攻击中。

合法网络扫描工具如 **Advanced Port Scanner** 和 **IP Scanner** 用于生成 IP 和设备名称列表，允许攻击者进入受害者最重要的计算机和基础设施。

误用合法的 **AnyDesk** IT 管理工具越来越常见，因为它允许攻击者直接控制目标计算机，包括控制鼠标/键盘和查看屏幕。合法远程访问服务如 **TeamViewer**、**Screen Connect**、**Atera RMM** 和 **Splashtop** 也在 2021 年进入前列。

Process Hacker、**PCHunter** 和 **GMER** 都是包含内核驱动程序的合法工具。如果攻击者安装合适的内核驱动程序，通常可以禁用安全产品。

Microsoft Binaries

将 Microsoft 工具与普通工具区分说明了攻击者的新趋势。此类工具都由 Microsoft 签名。**PowerShell** (74%) 不出意料占据第一，之后是 **PsExec** (53%)，“**net.exe**” (28%)、“**rundll32.exe**” (27%) 和 **WMI Command-line** (WMIC) 工具 (22%)。相比 2020 年，PowerShell、PsExec 和 WMIC 的使用在 2021 年都增加。

“net.exe”工具用于攻击的多个阶段，最常见作为发现工具，而“rundll32.exe”大量用于执行和避开防御。

其他可能指向网络中潜伏攻击者的 Microsoft 工具包括“**whoami.exe**”、**Task Scheduler**（保持持久）和“**schtasks.exe**”（执行恶意代码）。应密切监测任何此类工具的使用。

其他制作物

此类包括工具和技术，例如尝试禁用防护，漏洞（如 ProxyShell），使用云服务如 **Mega.io**，其他发现的恶意软件，二次感染，以及使用的传输协议。

恶意脚本（不包括 PowerShell）在调查的事件中占 59%。恶意脚本指实现恶意活动的软件代码。攻击者误用的脚本示例包括 DOS/CMD 批处理和命令行脚本，Python 脚本（像程序一样执行的文件中的命令序列），以及 VBScript（可以在 Windows 或 Windows Explorer 中执行的 Visual Basic 脚本）。

Web shell 是第二常见的威胁（占事件的 38%），ProxyShell (28%) 和 ProxyLogon (11%) 也很广泛。安装服务，禁用防护，转储 LSASS，创建恶意帐户，修改注册表，清除日志占据前 10 的其余位置。

数据泄露

2021 年，**Rclone** 进入用于泄露的主要制作物列表。Rclone 是一个命令行工具，可以连接多个云存储提供商如 Mega，2021 年它是数据泄露中使用最广泛的工具。今年数据中的其他云存储提供商包括 **Dropbox**、**DropMeFiles**、**M247**、**pCloud** 和 **Sendspace**。

除了 Rclone，事件调查中协助数据泄露的工具还包括 **Megasync**、**FileZilla**、**Handy Backup**、**StealBit**、**WinSCP** 和 **Ngrok**。

考虑到所有调查事件的 38% 涉及泄露数据，2020 年为 27%，2021 年主要列表中的泄露工具排名并不意外。多个其他事件（整体 8%）显示收集数据并等待可能移除的迹象。证据表明，在发生泄露的案例中，失窃信息接下来在 46% 的事件中泄露。

攻击者通常移除信息，作为部署勒索软件前的最后阶段。Sophos 的事件分析显示，2021 年数据泄露与部署勒索软件之间时间中位数约 44 小时。平均时间略超过 4 天（4.28 天），时间中位数低于 2 天（1.84 天）。

无论采用哪种平均值，这里的要点在于泄露后，防御者有可能阻止最终同时最具破坏性的攻击阶段出现。因此，应优先调查发现的已知用于数据泄露的任何工具。

工具组合

事件调查显示受害者网络上的工具组合模式，为 IT 安全团队提供有力的警告信号（在一些案例中提供 2020 年对比数据）：

- 2021 年，PowerShell 和恶意非 PS 脚本组合占案例的 64%
- PowerShell 和 Cobalt Strike 组合占案例的 56%，2020 年为 58%
- PowerShell 和 PsExec 组合占案例的 51%，2020 年为 49%
- PowerShell、恶意脚本和 Cobalt Strike 组合占案例的 42%
- PowerShell、恶意脚本和 PsExec 组合占案例的 38%
- PowerShell、Cobalt Strike 和 PsExec 组合占案例的 33%，2020 年为 12%
- Cobalt Strike 和 Mimikatz 组合占案例的 16%

此类关联在今年的重要性和去年一样，因为侦测到它们可以作为攻击即将到来的预警，或者确认存在活跃攻击。

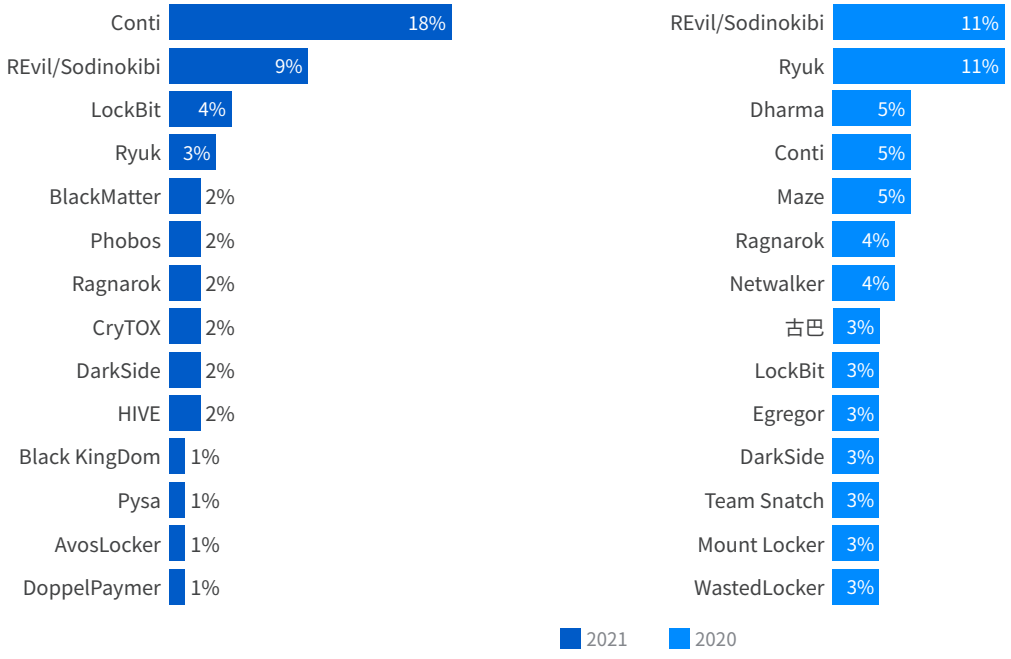
2021 年的主要勒索软件对手

分析包含的 144 个事件中确定了 41 个不同勒索软件对手。其中约三分之二 (28) 是 2021 年新报告的系列。2020 年事件中的 18 个恶意软件系列已经从 2021 年列表中消失，清楚表明网络威胁环境参与者数量众多、动态和复杂，以及防御者面临的难度。

从许多方面来看，2021 年都“属于”Conti，一个多产的 RaaS 运营商，在 Sophos 调查事件的五分之一 (18%) 都有出现。值得注意的是，虽然 REvil 勒索软件占总体事件的十分之一，但 2021 年 7 月似乎停止运行（2021 年 9 月短暂重新出现，2022 年再次出现）。

2021 年的其他流行勒索软件系列包括 DarkSide（美国 Colonial Pipeline 攻击背后的 RaaS），以及 Black KingDom，2021 年 3 月伴随 ProxyLogon 漏洞出现的“新”勒索软件系列之一。

归属：主要勒索软件对手



2021 年约四分之一 (24%)，2020 年 25% 的事件归属于其他勒索软件系列，其余事件无法确定划归到任何已知系列。

Sophos 已经深度报道了 Conti 勒索软件。可以在 Sophos 的 勒索软件威胁情报中心找到关于 Conti 和其他流行勒索软件（如 LockBit、Ryuk 等）的大量文章。

结束语

所有企业都是躲在某个角落的对手的目标，并且对手数量越来越不止一个。无论是网络钓鱼和金融欺诈，还是僵尸网络搭建者，恶意软件投放平台，加密货币矿机，IAB，数据盗窃，企业间谍，勒索软件等 – 如果存在网络的漏洞进入点，就存在攻击者寻找并且最终找到利用的可能。

在封闭暴露的进入点，并完全擦除攻击者为建立和保持访问权所做的一切工作前，任何人都可以尾随进入网络。而且很可能会。

安全团队可以通过监测和调查可疑活动，保护自己的企业。并不是始终能够轻易分辨善意和恶意。任何环境的技术（无论是网络还是物理环境）都有很大的用处，但单纯技术是不够的。人的经验和技能以及应对能力在任何安全解决方案中都至关重要。

2021 年的重大事件响应教训是对手如何快速深入抓住容易被利用且广泛传播的漏洞，导致更长的入侵和多个对手。对于防御者来说，这些教训意味着侦测、调查和响应已知对手工具集及技术的警惕比以往更加重要。

Sophos Rapid Response

本报告的结果基于 Sophos Rapid Response 调查事件的数据，这是由专门事件响应者和威胁消除专家组成的队伍。Sophos Rapid Response 服务为现有 Sophos 客户和非 Sophos 客户提供。

如果您遇到活跃事件，希望联系快速响应团队，请随时拨打下面的号码：

美国：+1 4087461064

澳大利亚：+61 272084454

加拿大：+1 7785897255

法国：+33 186539880

德国：+49 61171186766

英国：+44 1235635329

瑞典：+46 858400610

其他数据表格

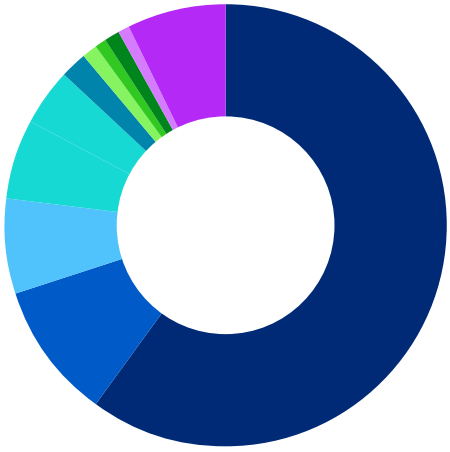
事件调查制作物与 MITRE 攻击链的对应

在 MITRE ATT&CK 框架中对应事件调查观察到的工具、技术和其他制作物。更多详细信息将发布在 Sophos News 的文章中。

MITRE 攻击阶段											
初始访问	执行	持续	权限提升	避开防御	凭据访问	发现	横向移动	收集	指挥控制	泄露	影响
制作物											
远程服务	PowerShell	Cobalt Strike	Mimikatz	PowerShell	Mimikatz	Advanced IP Scanner	RDP	网络浏览	Cobalt Strike	Rclone	数据加密
漏洞攻击	PsExec	AnyDesk	ProcDump	Rundll32.exe	ProcDump	Netscan	Cobalt Strike	Rclone	PowerShell	WinRAR	网络攻破

事件响应人口统计 2021

按国家划分的事件响应案例

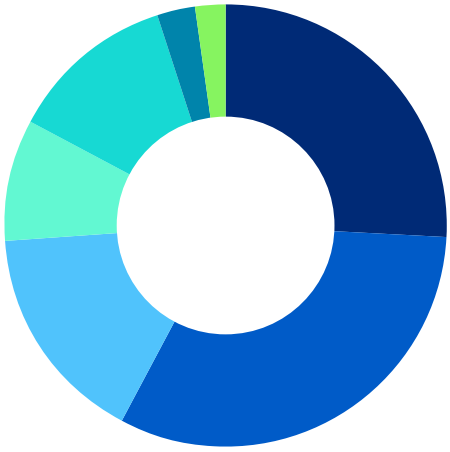


- 美国 60%
- 德国 10%
- 英国 7%
- 加拿大 6%
- 意大利 4%
- 西班牙 2%
- 法国 1%
- 瑞士 1%
- 比利时 1%
- 菲律宾 1%
- 其他 7%（荷兰、奥地利、阿联酋、沙特阿拉伯、巴哈马、安哥拉、日本）

按行业划分的事件响应案例

- 制造 17%
- 零售 14%
- 医疗 12%
- 信息技术 9%
- 建筑施工 8%
- 教育 6%
- 食品 4%
- 物流 4%
- 金融 4%
- 娱乐 3%
- 服务 3%
- 新媒体 3%
- 其他 13%（交通运输、制造、MSP/主机、非盈利性、政府、住宿、法律、农业、能源、房地产）

按企业规划（员工数量）划分的事件响应案例



- 1–100 **26%**
- 101–250 **32%**
- 251–500 **16%**
- 501–1000 **9%**
- 1001–3000 **12%**
- 3001–5000 **3%**
- 5000+ **2%**

中国（大陆地区）销售咨询
电子邮件：salescn@sophos.com

2022-05-25 ZHCN (DD)